Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Big Data and Consumer Privacy	)	Docket No. 140514424-4424-01
in the Internet Economy	)	RIN 0660-XC010

COMMENTS OF CTIA—THE WIRELESS ASSOCIATION®

Debbie Matties
Vice President, Privacy

Michael F. Altschul
Senior Vice President, General Counsel

CTIA-THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3654

August 5, 2014

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Big Data and Consumer Privacy	)	Docket No. 140514424-4424-01
in the Internet Economy	)	RIN 0660-XC010

COMMENTS OF CTIA—THE WIRELESS ASSOCIATION®

CTIA—The Wireless Association® ("CTIA") welcomes the opportunity to provide input to the Department of Commerce on issues raised in its request for public comment ("Request") on the White House Office of Science and Technology Policy's report on big data and privacy ("Big Data Report") and the report of the President's Council of Advisors on Science and Technology on technology, privacy and big data ("PCAST Report").[1] The Request seeks comment on, among other things, how the White House Consumer Privacy Bill of Rights ("CPBR")[2] could *both* support innovation that data-driven innovation makes possible *and* respond to privacy risks, as well as how a "responsible use" framework could be embraced within the CPBR.

I. INTRODUCTION

CTIA is an international nonprofit trade association that has represented the wireless communications industry since 1984. Its members develop and deliver a host of

---

[1] *Big Data and Consumer Privacy in the Internet Economy*, 79 Fed. Reg. 32714 (June 6, 2014) *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-06-06/pdf/2014-13195.pdf; Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) (''Big Data Report''), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[2] The White House proposed a Consumer Privacy Bill of Rights in 2012. *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* (Feb. 2012) ("White House Privacy Blueprint") *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

products and services that are part of the wireless ecosystem and rapidly developing network of connected devices.[3]

The convergence of mobile services, connected devices, cloud computing and data analytics is advancing society as a whole by creating jobs and driving economic growth, now and over the next decade. For instance, Cisco estimates the global business impact of connected devices and data analytics will reach $14.4 trillion by 2022, and Gartner forecasts that by 2015, data-driven innovation will create 4.4 million information technology jobs globally, 1.9 million of which will be in the U.S.[4]

In addition, consumers are benefiting from innovative uses of mobile device data, often in de-identified or aggregated form. For instance, mobile application developers have created mobile apps that aggregate and analyze cell phone location information with sophisticated analytical tools to identify and solve traffic problems by suggesting optimal driving routes to commuters.[5] In addition, civil engineers have started to use mobile phone data to discover patterns in urban road traffic that can inform the design of road

[3] CTIA – The Wireless Association® ("CTIA") is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization includes Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[4] *See* Joseph Bradley et al., *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, Cisco Systems, Inc. at 2 (2013), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf, and Software and Information Industry Association, *Data-Driven Innovation*, at 12 (2013) *available at* https://www.siia.net/index.php?option=com_docman&task=doc_download&gid=4279&Itemid=318. In addition, GSMA, a global trade association for the mobile industry, and Machina Research predict that connected devices will generate $4.5 trillion in global revenue by 2020. GSMA and Machina Research, *The Connected Life: A USD 4.5 Trillion Global Impact in 2020* (Feb. 2012), *available at* http://connectedlife.gsma.com/wp-content/uploads/2012/02/Global_Impact_2012.pdf.

[5] *See, e.g.,* Waze, https://www.waze.com/ (last visited Aug. 4, 2014). Waze is a mobile app that allows drivers to "share real-time traffic and road info, saving everyone time and gas money on their daily commutes." *Id.*

networks to reduce congestion.[6] Carriers also use analytics to mine diagnostic and network traffic data to identify and correct device and network problems, thereby improving services for their customers. For example, carriers analyze aggregated customer call information to identify confusing menu options and to improve customer service training. In addition, cell service providers identify coverage problems and improve network performance. They monitor dropped call logs in real time, correlating this with historical trends in order to locate and prioritize outages as soon as they occur. Carriers' use of data for these purposes does not raise privacy concerns, and consumers want and expect carriers to perform these services for them.

CTIA members are committed to safeguarding their customers' data. They have a strong track record of addressing privacy issues and have programs in place to protect personal information.[7] CTIA members recognize that strong privacy protection is a good business practice. They have incentive to earn and maintain consumer trust and loyalty by protecting their customers' data. CTIA members' interests are thus aligned in this area with their customers' interests.

U.S. privacy frameworks – whether they are in the form of legislation, self-regulatory principles, or best practices – should promote and protect consumers' privacy, while allowing companies flexibility to innovate in ways that benefit individual consumers and society as a whole. Big data analytics is part of the most recent wave of

---

[6] *See* Pu Wang, Timothy Hunter, Alexandre M. Bayen, Katja Schechtner & Marta C. Gonzalez, *Understanding Road Usage Patterns in Urban Areas*, Scientific Reports 2 (Dec. 20, 2012) *available at* http://bayen.eecs.berkeley.edu/sites/default/files/journals/srep01001.pdf.

[7] For example, CTIA used the Fair Information Practice Principles to develop the CTIA Best Practices and Guidelines for Location Based Services (Mar. 23, 2010) ("LBS Guidelines"), which are designed to promote and protect consumer privacy as new location-based services are created and deployed. The LBS Guidelines are available at http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf.

technological innovation that promises tremendous benefits to consumers and society across a range of industry sectors, including healthcare, education, energy, and transportation. CTIA members were encouraged that the Big Data Report stressed the importance of, and the White House's commitment to, the digital economy and the free flow of data that drives innovation. CTIA members view the CPBR as an important, flexible, and balanced framework for best practices that will protect consumers' privacy and foster data driven innovation.[8] Indeed, CTIA members have already incorporated applicable CPBR principles into their privacy practices.[9]

CTIA members believe that strong data security is a fundamental component of a comprehensive data privacy framework. Today's patchwork of state and federal information security and data breach notification requirements create inconsistent – and sometimes contradictory – responses to breaches that do not benefit consumers. They therefore support the administration's call for Congress to pass data security and breach notification legislation.[10]

If the administration also decides to submit omnibus consumer privacy legislation to Congress, CTIA members encourage the administration to clarify and appropriately limit the type of data that legislation would cover and to emphasize certain elements of the CPBR. In addition, any legislation codifying the CPBR should articulate a flexible "responsible use" framework that is supported by elements of the CPBR and includes, but does not mandate particular accountability mechanisms.

---

[8] Big Data Report at 39 (stating that the Obama Administration supports "America's leadership position in using big data to spark innovation, productivity, and value in the private sector").

[9] *See, e.g.,* LBS Guidelines at pp. 1, 5 (directing LBS companies to ensure transparency through "meaningful notice," to provide individual control by obtaining user consent and allowing users to revoke consent, and allowing use of location information consistent with consumers' expectations, which can be inferred from the context of the relationship with the consumer).

[10] Big Data Report at 62 (urging Congress to pass national data breach legislation).

II. DATA BREACH LEGISLATION WILL BENEFIT CONSUMERS AND BUSINESSES

CTIA supports federal data security and breach notification legislation that sets one national standard for all companies handling sensitive personal data. Today's patchwork of state and, in certain sectors, federal information security and data breach notification laws is often confusing to businesses and provides uneven protection for consumers.[11] A comprehensive, streamlined federal framework would create more certainty for businesses and better protect consumers from the harms associated with data breaches. Such legislation should be technology neutral, preempt state laws, and prohibit private rights of action.[12]

III. ANY OMNIBUS PRIVACY LEGISLATION SHOULD CLARIFY AND LIMIT THE DATA COVERED

If the administration submits omnibus privacy legislation to Congress, CTIA believes it should clarify and limit the type of data that legislation would cover. For instance, legislation should not cover network data that carriers use to protect their networks and improve performance. Nor should legislation apply to data collected from public sources. Many of the data points used in data-driven innovation are pulled from publicly available data, such as census information, that companies and researchers have been using for years. The Obama Administration has recognized the benefits of public data to researchers and should be commended for making valuable data publicly available for analysis through its Open Government Initiative and accompanying online platform,

---

[11] White House Privacy Blueprint at 39 (stating that the "patchwork of State laws creates significant burdens for companies without much countervailing benefit for consumers").

[12] Testimony of Debbie Matties, Vice President, Privacy, CTIA, House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade Hearing, *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?*, July 18 2013, *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Matties-CMT-Data-Breaches-Consumer-Protection-2013-7-18.pdf.

Data.gov. As the Administration has noted, access to raw data can unleash innovation and fuel the creation of applications that increase quality of life, improve energy efficiency, and spur economic growth.[13]

In addition, legislation should not cover aggregate or de-identified data. This approach would be consistent with the White House Privacy Blueprint, which encouraged companies to use data de-identification as a form of privacy protection, and the Federal Trade Commission's encouragement to use de-identification as a privacy best practice.[14] Indeed, at a recent roundtable discussion about the Internet of Things and big data, FTC Commissioner Julie Brill referred to recommendations that the FTC made in *Protecting Consumer Privacy in an Era of Rapid Change* (the "FTC Privacy Report")[15] when she urged developers to use data de-identification as a best practice to protect privacy.[16]

The FTC Privacy Report articulated certain steps that companies could take to de-identify data. Specifically, the FTC will not consider data to be reasonably linkable to a particular consumer or device if the company:

(1) Uses reasonable measures to de-identify the data;

(2) Publicly commits to (i) maintain and use the data in de-identified form and (ii) not attempt to re-identify the data; and

(3) Contractually prohibits third parties from attempting to re-identify the data.[17]

---

[13] *See* Data.gov, http://www.data.gov (last visited Aug. 4, 2014).

[14] White House Privacy Blueprint at 48 (urging companies to protect consumer privacy by "securely dispos[ing] of or de-identify[ing] personal data" no longer needed) (emphasis added).

[15] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[16] Julie Brill, Commissioner, FTC, Speech for the Center for Policy on Emerging Technology, The Internet of Things: Roundtable with FTC Commissioner Brill: *The Internet of Things: Building Trust to Maximize Consumer Benefits* (Feb. 26, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/203011/140226cpetspeech.pdf.

[17] FTC Privacy Report at 21.

Whether a company has taken "reasonable measures" to de-identify data will depend on the circumstances, including the available methods and technologies, the nature of the data at issue, and the purposes for which the data will be used.[18]

Recent academic research shows that the risk of re-identifying de-identified datasets is exaggerated.[19] Specifically, this research shows that critics of de-identification typically cite only to computer scientists who have technical expertise in data analysis and have been able to re-identify data by using sophisticated analytical tools.[20] The general public, however, does not possess this expertise or the motivation to re-identify large de-identified datasets.[21] Furthermore, because most datasets that would be necessary to re-identify individuals are not publicly available, strong administrative controls and data security safeguards make technical re-identification implausible.[22] Indeed, researchers have shown that "when proper de-identification methods have been used to effectively reduce re-identification risks to very small levels, it becomes highly unlikely that data intruders would conclude that it is worth the time, effort and expense to undertake a re-identification attempt in the first place."[23]

---

[18] *Id.*

[19] *See generally* Ann Cavoukian & Daniel Castro, Information and Privacy Commissioner Ontario, Canada, *Big Data and Innovation*, *Setting the Record Straight: De-Identification Does Work* (June 16, 2014), http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identification_ITIF1.pdf.

[20] Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1, 31-33 (2011) (citing a Netflix study where two sophisticated data scientists re-identified de-identified data about Netflix users' video preferences); *see also* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 117, 1126-1140 (2013) (arguing that data de-identification critics have made unwarranted assumptions about the "nature of privacy and [data] utility" and noting the availability of data de-identification techniques that preserve the utility of data while protecting privacy).

[21] *See* Yakowitz, *supra* note 20.

[22] *See* Ann Cavoukian and Daniel Castro, Big Data and Innovation, *supra* note 19, at p. 5 (stating that it is wrong to assume that the data necessary to re-identify individuals is available and that "an attacker could actually re-identify [de-identified data] in practice").

[23] Daniel Barth-Jones, *Does De-Identification Work or Not?*, FierceBigData.com (June 23, 2014), *available at* http://www.fiercebigdata.com/node/35502156 (citing to his three-part essay for Harvard Law School's *Bill of Health* Symposium on the Law, Ethics & Science of Re-identification Demonstrations); *see also*

Legislation should not apply to data that has been de-identified through robust de-identification techniques, such as those outlined in the FTC Privacy Report or other academic research. If legislation or regulators require perfect anonymity, consumers will not enjoy the potentially transformative social and economic benefits of data driven innovation.[24] Therefore, companies need flexibility to weigh the potential risks of re-identification against the potential benefits to consumers and society when they use de-identified data. This approach is consistent with aspects of the FTC's analysis under the "unfairness" doctrine, which weighs consumer injury against consumer benefits.[25] Where the risk of re-identification is extremely low or merely theoretical – because the resources necessary to re-identify the data are high, the incentives to do so are low, or the data is not available to the public – and the potential benefits of big data analysis are high, regulation should not prevent the use of that data for data-driven innovation.[26]

IV. ANY PROPOSED LEGISLATION SHOULD EMPHASIZE CERTAIN CPBR PRINCIPLES

The traditional "notice and choice" framework that has long governed consumer privacy may not address the use of big data in all circumstances and therefore should be reinforced by other CPBR principles, when appropriate. Under the traditional Fair

---

Southern Illinoisan v. Dep't of Public Health, 349 Ill. App. 3d 431 (Ill. App. Ct. 5th Dist. 2004) (holding that the release of de-identified data from Cancer Registry would not tend to reveal the identity of individuals even though plaintiffs produced evidence that data science expert had been able to re-identify individuals, where plaintiffs had not shown that the general public, as opposed to an expert in data science, could re-identify data), *aff'd* 218 Ill. 2d 390 (2006).

[24] *See* Daniel Barth-Jones, *supra* note 20.

[25] The FTC considers three factors when applying the FTC Act prohibition against unfairness: (1) whether the practice injures consumers; (2) whether it violates established public policy; and (3) whether it is unethical or unscrupulous. FTC, FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness. The consumer injury prong will be met only if the FTC finds that the injury (a) was substantial (and not speculative or subjective), (b) was not outweighed by offsetting consumer benefits (including the impact on incentives to innovate), and (c) could not reasonably have been avoided. *Id.*

[26] *See* Daniel Barth-Jones, *supra* note 20.

Information Practice Principles ("FIPPs")-based privacy framework, companies are expected, at the time of data collection, to give consumers notice of (among other things) the data they collect, the purpose for which they collect it, and the entities with whom they will share it. Companies are expected to use the data only for those purposes for which they collected the data, and they are expected to offer consumers choices about how their information may be used for secondary purposes.

One of the defining characteristics of data-driven innovation, however, is that companies will not always be able to predict at the time of collection all of the possible beneficial uses of data that they may discover in the future.[27] In addition, non-consumer facing companies that increasingly obtain large amounts of consumer data are not in a position to interact directly with, and provide notice and choice to, consumers. The White House recognized this trend in its Big Data Report, which noted that "the trajectory of technology is shifting to far more collection, use and storage of data by entities that do not have a direct relationship with the consumer or individual."[28]

Requiring companies to identify consumers they do not know could deter companies from innovating, denying consumers and society the potentially transformative benefits of data-driven innovation.[29] Requiring companies to contact consumers to update their consent each time they use data for a new purpose similarly

---

[27] Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 153 (2013).

[28] Big Data Report at 55-56; *see also* FTC, *Data Brokers: A Call for Transparency and Accountability*, at 49 (May 2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (noting that data brokers, which collect a tremendous amount of data about consumers, are not consumer facing companies).

[29] *Cf.* Mayer-Schönberger & Cukier at 173 (stating that "when much of data's value is in secondary uses that may have been unimagined when the data was collected, [a notice and choice framework] is no longer suitable").

could prevent companies from launching new services. In addition, frequent notices in the context of ubiquitous data collection and big data analytics likely would be unhelpful, burdensome, and intrusive to consumers and would impede the delivery of the data-driven products and services consumers want.[30] "Notice and choice" therefore may be better expressed through the interplay of particular CPBR principles – namely, "respect for context," "transparency," and "individual control" – which together ensure consumers' privacy is protected and give companies the flexibility to innovate.

A. Respect for Context

The "respect for context" principle provides that consumers can expect companies to "collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[31] Because it gives consumers assurance that companies will use data consistent with consumers' expectations, this principle can stand in the place of the FIPPs principles of "purpose specification" and "use limitation." This principle also serves as a useful guidepost and limitation in the big data environment, where it can fill some of the gaps left by notice and choice.

As the White House Privacy Blueprint explained, the "respect for context" principle allows changes in the relationship between the consumer and the company "over time in ways not foreseeable at the time of collection," and enables "adaptive uses of personal data [that] may be the source of innovations that benefit consumers."[32] For instance, companies should be able to infer consent to collect and use personal data that is necessary to provide the service consumers request and to enhance and improve those

[30] Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes* 3-4 (Nov. 2012).

[31] White House Privacy Blueprint at 1.

[32] *Id.* at 16.

services in ways unforeseeable at the time of data collection.[33] Requiring consumers to regularly check privacy policies, which can be updated frequently, and provide separate consent for subsequent data use is impractical and would limit the functionality and economic benefits of data-driven innovation.[34]

B. Transparency

Greater awareness about data collection and use will improve consumer trust, establish consumer expectations, and reduce the risk of consumer surprise. As companies develop new products and services, including those that relate to the Internet of Things, it may be necessary to find new ways to disclose data practices that matter to consumers.

Some kinds of notices are more effective than others. Companies therefore should determine what kinds of notices will have the most impact on consumers while also having the flexibility to avoid creating notice fatigue. For example, companies could look for guidance to methods that Ilana Westerman, founder of digital design firm Create with Context, has developed to ensure that privacy notices maximize consumer understanding and awareness of data flows and build consumer trust.[35] Westerman's approach of designing products and services in a way that provides consumers the most appropriate and effective notice possible is consistent with the FTC's recommendation that engineers use "privacy by design" principles as they develop new products.

---

[33] *Id.* at 17-18.

[34] Cate & Mayer-Schönberger at 3.

[35] These principles include, but are not limited to, the following: (1) design user interfaces to inform consumers about data collection and use at the moment that they will care the most; (2) provide easy access to key information, recognizing that consumers are not motivated to dig through layers of policies online; (3) explain clearly what happens when users change privacy controls, including the value proposition for certain decisions; (4) display information the same way every time and in all locations; and (5) communicate to consumers that they are "known" to you when they have taken steps to remain logged into the service or when they have chosen to hide their identity from other users. *See* Create With Context, http://createwithcontext.com/insights-digital-trust-and-privacy.php (last visited Aug. 4, 2014).

In addition to notifying consumers about data practices in the traditional way (*i.e.,* through different kinds of company privacy notices directed at the company's customers), companies should ensure "transparency" by broadly promoting general consumer awareness of new data flows and their beneficial uses. Companies have the most knowledge about how they intend to use data and are in a good position to educate consumers about these issues. In addition, government agencies have historically played an important role in supporting industry efforts to foster greater consumer awareness and would help build greater consumer trust by continuing their role. For example, the FTC has a long established precedent of educating consumers about how to protect themselves in the marketplace. The Federal Communications Commission ("FCC") Consumer and Governmental Affairs Bureau has similarly played a role in educating the public about issues associated with mobile devices. Financial and health regulatory agencies also regularly provide guidance and host dialogues with consumers and educators about innovative uses of data, including big data analytics.

Broadly disseminated information can promote "transparency" by creating general consumer awareness about how new devices work and how they collect, use, and share personal data. Greater consumer awareness, in turn, will create a climate of trust between consumers and industry, and it will help consumers develop implicit expectations about data flows when using services online and in the Internet of Things. Increased consumer awareness of data practices can complement companies' traditional privacy notices, which consumers can continue to use to educate themselves about how industry sectors and individual companies use and protect personal data.

C. Individual Control and Individual Responsibility

"Individual control" is a flexible principle under which consumers can make informed decisions about data use, consistent with the scale, scope and sensitivity of the data. This principle encourages individual consumers to control their data by exercising personal responsibility. As the White House Privacy Blueprint explained, "[c]onsumers have certain responsibilities to protect their privacy as they engage in an increasingly networked world."[36]

The context in which companies collect and use data will affect the degree of "individual control" consumers have. When it is not practical for consumers to exercise control, companies can implement other elements of the CPBR in ways that protect consumer privacy.[37] For instance, consumers understand that an app that provides suggestions for nearby restaurants depends on access to one's geolocation data in order to function properly. It would not be desirable to the consumer to receive just-in-time notice and choice before the app accessed geolocation data for the purpose of providing recommendations, as such notice would create unnecessary friction in the user experience and over time de-sensitize the consumer to any valuable consumer protection.

Moreover, because companies will not know all of the future beneficial uses of data at the time of collection, other CPBR principles may play a more prominent role in an era of big data. "Transparency" and "respect for context," for instance, can create consumer awareness and implicit expectations that inform consumer consent to uses of

[36] White House Privacy Blueprint at 9.
[37] Cate & Mayer-Schönberger at 15.

data, while at the same time ensure uninterrupted data flows, enabling companies to use data-driven innovation effectively to provide seamless services to consumers.[38]

Any proposed legislation should follow the balanced approach that the White House took in the White House Privacy Blueprint, which called for "*appropriate* levels of transparency and individual choice" before data is re-used for a purpose unrelated to the purpose for which it was collected.[39] This approach will ensure that companies have the flexibility to use big data to innovate and provide consumers with new products and services that improve quality of life, while at the same time protecting their privacy.

V. ANY LEGISLATION SEEKING TO CODIFY THE CPBR SHOULD DEPEND ON A "RESPONSIBLE USE" FRAMEWORK

A legislative framework that emphasizes "responsible use" and uses that concept to inform the applicability of the other CPBR principles is well suited to protecting privacy and ensuring innovation in an era of big data.

This approach has many benefits. A "responsible use" framework is appropriate for an era of data-driven innovation and likely to protect consumers because it requires companies to use data responsibly throughout the period that they hold the data, rather than rely heavily on notices to consumers about their data practices. Moreover, unlike the current contract-based model, it also emphasizes the role of non-consumer facing companies in protecting personal privacy. A "responsible use" framework would ensure that privacy protections would not impede data-driven innovation. It properly puts the

---

[38] *See* Farhad Manjoo, *You Have To Buy This Ingenious Thermostat*, Slate Magazine (Oct. 2, 2012) *available at* http://www.slate.com/articles/technology/technology/2012/10/nest_thermostat_the_ingenious_heating_and_cooling_system_keeps_getting_smarter_.html (explaining the way that the Nest thermostat will collect and analyze data in real-time to improve the functionality of the device and consumers' experiences over time).

[39] White House Privacy Blueprint at 16 (emphasis added).

focus on what legitimizes data processing activity and gives companies the flexibility to collect data for a variety of applications that may not be apparent at the time of collection. Finally, a "responsible use" framework would allow companies to use de-identified data in ways that will maximize both privacy protection *and* the consumer and societal benefits of big data analysis.[40]

The Big Data Report recognized the rapid pace of technological innovation and the evolving nature of company-customer relationships. Industry practices and permissible uses of data should evolve in tandem. In this regard, legislation articulating a "responsible use" framework should incorporate a flexible risk-benefit approach that allows companies to evaluate the type of data involved, the potential beneficial use of the data, the potential privacy impact, and the risk of harm.

The Big Data Report discussed hypothetical situations in which big data analytics could create risks of harm to consumers. According to the Report, consumers could be harmed when inaccurate data is used to make decisions about their eligibility for – among other things – employment, insurance, education, and housing. The Report also posited that consumers could be harmed when companies use data to make inferences about sensitive personal characteristics, such as ethnicity, religion and gender.

Although the Report raised concerns about potential harms arising from specific uses of big data, CTIA members have not experienced this with their customers. To the extent that substantial consumer harms associated with big data arise, the existing legal regime of civil rights laws and consumer protection laws, such as the Fair Credit Reporting Act ("FCRA") and the Equal Credit Opportunity Act ("ECOA"), can

[40] Indeed, using data to segment consumers can be beneficial when, for example, it allows companies to send Latino consumers marketing materials and disclosures in Spanish.

supplement a "responsible use" framework to address inappropriate uses of, and potential consumer harms associated with, big data analytics. For example, a company that used big data analysis to segment and target low-income consumers for predatory lending purposes would be subject to liability under the Fair Housing Act or the ECOA.[41]

Additionally, the implementation of CPBR principles, such as the "respect for context," "transparency," and "access," and "accuracy" principles, already serves to protect consumers from data-driven innovation that could cause unintended harm. For instance, companies that use algorithms to score consumers' eligibility for certain resources (such as housing and credit) should allow consumers to access and correct inaccurate data, thereby ensuring consumers have due process in these determinations.

In some cases, review of the results of algorithmic decision-making may be useful to ensure compliance with civil rights and consumer protection laws. This approach would be consistent with the "Civil Rights Principles for the Era of Big Data," which a coalition of civil rights groups issued earlier this year.[42] The coalition did not oppose the use of big data analytics in decision-making, but rather urged companies to use big data applications in ways that ensure equal opportunity.[43] If documented instances of substantial consumer harms associated with big data analytics arise that are not addressed by the CPBR principles or consumer protections afforded by existing laws, all relevant

---

[41] Claims regarding predatory lending (e.g., racially targeted lending or "reverse redlining") generally are cognizable under the Fair Housing Act, 42 U.S.C. § 3605 *et seq.*, and the ECOA, 15 U.S.C. § 1691 *et seq*. *See, e.g., Matthews v. New Century Mortg. Corp.*, 185 F.Supp.2d 874, 886-87 (S.D. Ohio 2002); *Hargraves v. Capital City Mortg. Corp.*, 140 F. Supp.2d 7, 20-22 (D.D.C. 2000). In addition, ECOA and its implementing regulation (Regulation B) prohibit creditors from requesting *or collecting* information about an applicant's race, color, religion, national origin, or sex, unless an exception applies. 12 C.F.R. § 1002.5.

[42] *Civil Rights Principles for an Era of Big Data*, The Leadership Conference (Feb. 27, 2014) (stating that "[i]ndependent review" may be necessary to ensure that "[c]omputerized decisionmaking in areas such as employment, health, education and lending" is conducted fairly) *available at* http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.

[43] *Id.*

stakeholders should work to develop solutions. In the absence of such instances, the industry's incorporation of the CPBR principles and existing laws – such as FCRA, the Federal Trade Commission Act, and civil rights laws – provide consumers with ample protections.

VI. A "RESPONSIBLE USE" FRAMEWORK SHOULD EMPHASIZE ACCOUNTABILITY, BUT LEGISLATION SHOULD NOT MANDATE PARTICULAR MECHANISMS

Because it is hard to determine all of the possible uses of data at the time of collection, a "back end" mechanism could be used to consider the issues (such as consumer awareness, control and harm) potentially associated with secondary use of data. Accountability mechanisms that assess the impact of secondary uses of data will protect consumers *and* allow companies to develop new, beneficial uses for data that are not foreseeable at the time of collection.[44] CTIA members support the use of internal administrative controls and self-regulatory mechanisms that ensure oversight and enforcement of privacy programs and the use of big data.

Companies and academics are experimenting with and proposing new models of accountability and different kinds of internal and external use controls. CTIA members do not endorse any particular technology or methodology because this area is evolving, and it is too early to do so.[45] Consumer demand and other market forces will determine

---

[44] *See* Mayer-Schönberger & Cukier at 173-75 (stating that accountability mechanisms, rather than a "notice and consent" mechanism, are necessary to protect consumers and allow innovation in an era of "big data").

[45] *See* Jules Polonetsky & Omer Tene, *The Facebook Experiment: Gambling? In This Casino?*, Re/Code.net (July 2, 2014), *available at* http://recode.net/2014/07/02/the-facebook-experiment-is-there-gambling-in-this-casino (asserting that in an era of "big data," "[e]stablishing a process for ethical decision-making is key to ensuring that the benefits of data exceed their costs" and noting that companies have begun to do so through chief privacy officers and internal ethical review programs); *see also* Daniel Solove, *Facebook's Psych Experiment: Consent, Privacy, and Manipulation*, Huffington Post Blog, (June 30, 2014, 5:19 PM), *available at* http://www.huffingtonpost.com/daniel-j-solove/facebook-psych-

the optimal approach among the various possible accountability solutions, such as internal review boards, industry review boards, revised data use disclosures, data ethics officers, and privacy officers. Mandating particular accountability solutions would be premature at this point. Instead, CTIA recommends that the Administration start a dialogue to consider the state of existing accountability mechanisms and how they can be used or improved to maximize responsible use.

VII. OTHER ELEMENTS OF POTENTIAL LEGISLATION

CTIA members believe that any privacy and security legislation should fully preempt state laws and regulations and should be harmonized with existing sector-specific privacy and security laws. In addition, legislation should authorize federal civil law enforcement, backed up by civil law enforcement by state attorneys general as needed, and it should not provide a private right of action. Finally, legislation should provide a safe harbor for companies that follow the data de-identification methods that the FTC outlined in its 2012 Privacy Report and that encrypt personally identifiable information, as appropriate.

VIII. CONCLUSION

Big data technologies will create new opportunities to transform healthcare, education, energy, transportation, and more, enhancing the way we live and work. An essential component of consumer privacy protection is a uniform federal data security and breach notification law. Should policymakers decide to propose comprehensive privacy legislation, CTIA members encourage them to take a flexible and balanced approach that will avoid stifling the promise of big data. Omnibus legislation should not

---

experiment_b_5545372.html (noting the limitations of the approach taken by the internal review board that approved Facebook's decision to examine the effect that News Feed content had on users' moods).

apply to data that is de-identified or publicly available. It should include a "responsible use" framework that gives companies the flexibility to implement the CPBR principles, as appropriate, to allow subsequent, unanticipated uses of data that can benefit consumers and society. Existing civil rights and consumer protection laws can address harm to consumers if companies using big data analytics make sensitive or inaccurate inferences about consumers that affect their eligibility for employment, insurance, education, or housing. In the absence of actual harms to consumers, however, a flexible legislative approach supplemented by appropriate accountability mechanisms will ensure that consumers can enjoy the benefits of data-driven innovation while trusting that their privacy is protected.

Respectfully submitted,

/s/

Debbie Matties
Vice President, Privacy

CTIA-THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-3654

August 5, 2014